Alexander Wiegman

Security Engineer / Data Security Analyst
California, United States | **Email**: alex@madicetea.me | **Phone**: 209-353-5377 |
LinkedIn: https://www.linkedin.com/in/mrlogicalalex

Summary

- **8+ years of experience** as a **cybersecurity engineer** and **data security analyst**.
- Seeking **full-time** and **contract** opportunities.
- **Work authorization**: **United States (US) citizen.**

Key Skills and Competencies

- **Alerting**: Grafana, Prometheus, OpsGenie, ServiceNow, Slack (API Applications)
- **Cloud, Container, and Endpoint Security Monitoring**: AWS GuardDuty, CrowdStrike, Malwarebytes ThreatDown (Malwarebytes Nebula), Microsoft Defender for Cloud, Prisma Cloud, Qualys, SentinelOne, Snyk.io
- **Compliance Endpoint Monitoring**: Drata, Intune, JAMF, Vanta Security
- **Dashboards and Visualization**: Amazon QuickSight, Excel, Kibana, JIRA, PowerBI, Redash
- **Identity & Access Management (IAM) Administration**: AWS IAM, Azure Entra, Google Workspace
- **Identity Provider (IdP) authentication**: Amazon Cognito OIDC, AWS IAM Identity Center, Azure Active Directory, Google Workspace SAML, OKTA SSO
- **Incident Detection and Pattern Recognition**: Google BigQuery SQL, Kibana, Lucerne, Splunk
- **Incident Post-Mortem [Root Cause Analysis] Report Writing**: AWS PHD, Blameless
- **Script Writing**: AWS CloudShell, Azure CLI, Google Cloud CLI, Python, SQL
- **Threat Signature Trend Analysis and Writing**: Snort signature, Spamhaus DNS definitions, YARA rules

Certifications

- **AWS Certified AI Practitioner, Cloud Practitioner, Solution Architect (Associate)** | Obtained 2024
- **CompTIA Certified Security+, Network+** | Obtained 2022
- **Microsoft Certified Azure System Administrator** | Obtained 2021
- **CompTIA Certified CDIA+, Mobility+, A+** | Obtained 2017

(currently in process: AWS Certified Security – Specialty, Red Hat Certified Systems Administrator RHCSA, and ISC^2 CISSP)

Work Experience

Cloud Security Engineer

Amazon Web Services (AWS), Amazon Inc. – *Remote, USA* | **June 2023 – (Current)**

- Coordinated 200 investigatory and compliance requests across **15 AWS security services**, including **AWS CloudTrail**, for **high-value corporate** and **government** clients, achieving a 99% resolution rate within the target SLA.
- Served as the team's lead **Subject Matter Expert (SME)** for **AWS Artifact**, **AWS GuardDuty**, **AWS IAM Identity Center** and **AWS Inspector**, resolving all escalated issues within 36 hours and reducing resolution time by 3 days.
- Assessed AWS technologies and open-source solutions, such as **Temporary Elevated Access Management (TEAM)** and **Amazon Inspector Vulnerability Database for CVEs**, against client requirements, ensuring comprehensive protection and alignment with best practices, such as advising on how to 100% meet **CIS Benchmark standards**.
- Revamped the **security review process**, reducing the average response time for customer inquiries by **1 working day** from 3 days to 2 days.
- Identified and escalated ten **technical bugs** and five **localization errors** based on customer feedback, enhancing accuracy through continuous monitoring and improvement.
- Co-developed five granular actions in **AWS IAM**, providing customers with fine-grained access controls beyond default managed policies, aligning with secure architecture principles.
- Led cross-functional collaboration with Product Management for three **feature request** initiatives, utilizing data queries from over 2,000 AWS customers to support feature implementation and enhance cloud security solutions.

Information (GRC) Security Administrator

Blameless, Inc. – *Remote, USA* | **May 2022 – January 2023**

- Built **single sign-on (SSO)** integration of **Whistic third-party risk management** into our **Salesforce** tenant, optimizing the accessibility of customer trust **Pentest reports** & **SIG-LITE questionnaires** for Sales and Legal teams.
    - This expedited the pre-sales cycle by up to one week and led to a revenue increase of $25+ million in ARR.
- Architected and managed **endpoint device management** systems (**Drata** compliance monitoring, **Google Workspace DLP, JAMF** & **Intune MDM**, and **SentinelOne EDR**) across 300+ devices and 100 users to ensure 100% compliance with **AICPA SOC 2 Type 1** and **ISO 27001:2022** standards.
- Constructed **DoControl** automated security action (**SOAR**) workflows for **insider threat alerting**, **PII exposure**, and **Data Loss Prevention**, which reduced time to initial response for identified security incidents by 3-6 hours.
- Configured Identity and Access Management (IAM) in **Azure Active Directory** and **Google Workspace** for 80+ employees, managing authentication mechanisms, reinforcing security protocols, and defining user access controls.
- Composed & communicated official **public-facing status messages** for the Security team during two (2) critical **security incidents**, ensuring **GDPR** and **CCPA/CPRA** regulatory adherence.
- Established an annual **Security & Privacy Awareness program**, utilizing **KnowBe4** for training and executing semi-annual **phishing simulations**, which improved organizational phishing awareness from below 50% to mid-70s%.
- Directed a comprehensive monthly **internal audit program**, coordinating with all teams and management to mitigate organizational risk through access control audits, security **vulnerability reviews** in **Synk.io**, and audit trail monitoring. During my tenure, this led to a 25% reduction in security risks identified between my first and my last monthly audit.

Information (GRC) Security Analyst

Kong, Inc. – *Remote, USA* | **September 2021 – May 2022**

- Led and passed a **SOC 2 Type 2 audit** with **125 controls** over an accelerated 5-week period & co-presented an **ISO 27001:2013 assessment**, enhancing customer trust and aligning policies in alignment with industry standards.
- Deployed **CrowdStrike Endpoint Detection and Response (EDR)**, **Azure Active Directory, Splunk Security Information and Event Management (SIEM)** log analysis tooling, and **Drata** for automated compliance across 600+ endpoints.
- Constructed **Proofpoint Data Loss Prevent (DLP)** rules to manage sensitive information in email systems, which scanned over 5,000 emails daily.
- Developed and implemented the "Document Sharing and Security Questionnaire" policy, which incorporated 400 responses from the **SIG-LITE questionnaire** and defined target SLA of no more than 5 days for custom questionnaires.
- Integrated **OKTA SAML Single Sign-On** with our **OneTrust compliance** software suite.
- Authored and iteratively optimized a **JIRA change management workflow** across the Company, resulting in a 330% increase in compliant changes and improving operating efficiency by 3 hours / week.
- Collaborated with **Legal** and **Executive Management** to ensure compliance with the **Personal Information Protection Law (PIPL)**, as a responsible member for the opening of a new office location in China.
- Designed and maintained 3 monthly **JIRA visualization dashboards and filtered reports**, providing actionable insights to corporate leadership and enhancing data-driven decision-making.

Senior Security Operations Analyst

PerimeterX, Inc. – *San Mateo, California, USA; Remote, USA* | **November 2019 – September 2021**

- Guided hundreds of customers regarding **HTTP data logging**, **AIO (All-In-One) Bot software** detection parameters, **JavaScript supply-chain risk** analysis, and our **integrations** with **Apache, Node.JS, Fastly, and AWS Lambda**.
    - Achieved 99% satisfaction ratings through several thousand customer interactions.
- Designed and deployed 30 automated alerting rules using **Prometheus**, and **Grafana** for visualization.
- Developed **Slack API app** alerting with YAML, JavaScript, and Python, which enhanced **time to first response** capabilities for our threat detection by 20-60 minutes per incident.
- Automated and optimized 20 **SQL queries** with dynamic data parameters in **Redash**, leading to a 40%-75% increase in efficiency and a 250% improvement in usability for customer-facing departments. Additionally, **Redash visualizations** were used in quarterly business reports, which directly facilitated up-sell agreements of up to 550%.
- Collaborated with R&D, Product, Solutions Architecture, Customer Success, and Sales teams to develop almost one thousand AI-learning pattern detection **YARA rules** in our **rapid7 SIEM** for account takeover, card testing, and other **Indicators of Compromise (IoC)**. Even today, these rules continue to process billions of API requests each hour.

Security Researcher

Pipeline, K.K. – *Ningyocho, Tokyo, JP* | **February 2019 – July 2019**

- Recorded 100s of observations of APAC regional **C2 server** & **DNS resolver vulnerabilities** using **Spamhaus** partner **SIEM** data, configuring secure policies, and updating **cloud-hosted containers** to enhance overall security posture.
- Architected and deployed an internal corporate **BIND DNS server** with **Response-Policy Zones** to support **SIEM data ingestion** and managed logging visualization data in **Elastic Logstash Kibana (ELK)**.
- Delivered **critical production support** to three client companies, driving a notable 200% increase in upsell revenue for one client. This support involved **applying endpoint security management tools** and **optimizing client systems** for better performance and security.
- Resolved a **false-positive spam listing** issue linked to nameservers of a shared hosting provider, achieving a **recovery time objective (RTO)** of one business day. Conducted a thorough **root-cause analysis** and implemented corrective measures to restore **highly available** and reliable **email security** and website communications.
- Led cost-saving initiatives by managing **secure data destruction** and upgrading our OS licensing and authentication to **Azure Active Directory**. These risk and compliance actions resulted in **operational savings** of 750,000+ Japanese yen.

Data Security Analyst

Junction Ltd. – *Shibuya, Tokyo, JP* | **October 2016 – May 2017**

- **Identified a critical security vulnerability** in an event signup form & ensured protection of millions of form responders' data by **responsibly disclosing** the issue to the signup form hosting company's security team.
- Co-authored and published the Junction Tokyo 2017 event website, leveraging expertise in **web development and security** to ensure compliance with data protection standards.
    - Developed and administered **WordPress website backends**, including the implementation of **security plugins**, **SSL/TLS certificates**, and adherence to **European and Finnish digital security regulations**.
- Collaborated with the social networking team to secure our communication channels with **multi-factor authentication (MFA)**, while also creating updates on Twitter (now X) and Slack for website and event promotion.
- Managed **network security** and **physical security** measures during the event, conducting **data forensics** and overseeing the protection of sponsor demo areas through effective security controls.
- **Archived** the event website and development project in the **Internet Archive Wayback Machine**.

Other Roles Held

University of Tokyo	- **Faculty Development Curriculum Researcher**	| September 2018 – February 2020
	- **Remote Sensing Engineering Researcher**	| September 2018 – August 2019
	- **Professional Ethics Course Lecturer**	| September 2018 – December 2018
	- **Biology Lab Teaching Assistant**	| January 2018 – February 2018

Education

Master's degree in Information Science *(MLIS)*

San Jose State University – *San Jose, California, USA* | **June 2023 – (Current)**

Selected Coursework: Database Management and Indexing Systems, Information Security & Risk Assurance, Red Hat Linux Administration, SQL Programming, US Government Information Systems

Bachelor's degree in Environmental Science with ***minors*** in Information Science & Science and Technology Studies

University of Tokyo – *Komaba, Tokyo, JP* | **September 2015 – September 2019**

Selected Relevant Coursework: Android Application Development, Artificial Intelligence and Statistical Machine Learning for Engineering Students, Compilers, Computer Architecture, Database Management Systems with SQL, Deep Learning with Python, Human Impacts on Artificial Intelligence, Mathematical Modelling and Simulations with MATLAB, Neural Networks in Remote Sensing, OpenCV with C++, Operating Systems